U. S. Department of Health and Human Services
U. S. Food and Drug Administration
Center for Food Safety and Applied Nutrition
March 21, 2003

GUIDANCE FOR INDUSTRY

RETAIL FOOD STORES AND FOOD SERVICE ESTABLISHMENTS: FOOD SECURITY PREVENTIVE MEASURES GUIDANCE

This draft guidance represents the Agency's current thinking on the kinds of measures that retail food store and food service establishment operators may take to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public.

Purpose and Scope:

This draft guidance is designed as an aid to operators of retail food stores and food service establishments (for example, bakeries, bars, bed-and-breakfast operations, cafeterias, camps, child and adult day care providers, church kitchens, commissaries, community fund raisers, convenience stores, fairs, food banks, grocery stores, interstate conveyances, meal services for home-bound persons, mobile food carts, restaurants, and vending machine operators). This is a very diverse set of establishments, which includes both very large and very small entities.

This draft guidance identifies the kinds of preventive measures they may take to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions. Operators of food retail food stores and food service establishments are encouraged to review their current procedures and controls in light of the potential for tampering or other malicious, criminal, or terrorist actions and make appropriate improvements.

This draft guidance is designed to focus operator's attention sequentially on each segment of the food delivery system that is within their control, to minimize the risk of tampering or other malicious, criminal, or terrorist action at each segment. To be successful, implementing enhanced preventive measures requires the commitment of management and staff. Accordingly, FDA recommends that both management and staff participate in the development and review of such measures.

Limitations:

Not all of the guidance contained in this document may be appropriate or practical for every retail food store or food service establishment, particularly smaller facilities. FDA recommends that operators review the guidance in each section that relates to a component of their operation, and assess which preventive measures are suitable. Example approaches are provided for many of the preventive measures listed in this document. These examples should not be regarded as minimum standards. Nor should the examples provided be considered an inclusive list of all potential approaches to achieving the goal of the preventive measure. FDA recommends that operators consider the goal of the preventive measure, assess whether the goal is relevant to their operation, and, if it is, design an approach that is both efficient and effective to accomplish the goal under their conditions of operation.

Structure:

This draft guidance is divided into five sections that relate to individual components of a retail food store or food service establishment operation: management; human element – staff; human element – public; facility; and operations.

Related Guidance:

FDA has published two companion guidance documents on food security, entitled, "Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance" and "Importers and Filers: Food Security Preventive Measures Guidance" to cover the farm-to-table spectrum of food production. Both documents are available at: http://www.access.gpo.gov/su_docs/aces/aces140.html.

Additional Resources:*

A process called Operational Risk Management (ORM) may help prioritize the preventive measures that are most likely to have the greatest impact on reducing the risk of tampering or other malicious, criminal, or terrorist actions against food. Information on ORM is available in the Federal Aviation Administration (FAA) System Safety Handbook, U.S. Department of Transportation, FAA, December 30, 2000, Chapter 15, Operational Risk Management. The handbook is available at: http://www.asy.faa.gov/Risk/SSHandbook/Chap15_1200.PDF.

The U.S. Department of Transportation, Research and Special Programs Administration has published an advisory notice of voluntary measures to enhance the security of hazardous materials shipments. It is available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-3636-filed.pdf. The notice provides guidance to shippers and carriers on personnel, facility and en route security issues.

---

* Reference to these documents is provided for informational purposes only. These documents are not incorporated by reference into this guidance and should not be considered to be FDA guidance.

The U.S. Postal Service has prepared guidance for identifying and handling suspicious mail. It is available at: http://www.usps.com/news/2001/press/mailsecurity/postcard.htm.

The Federal Anti-Tampering Act (18 USC 1365) makes it a federal crime to tamper with or taint a consumer product, or to attempt, threaten or conspire to tamper with or taint a consumer product, or make a false statement about having tampered with or tainted a consumer product. Conviction can lead to penalties of up to $100,000 in fines and up to life imprisonment. The Act is available at: http://www.fda.gov/opacom/laws/fedatact.htm.

The National Infrastructure Protection Center (NIPC) serves as the federal government's focal point for threat assessment, warning, investigation, and response for threats or attacks against U.S. critical infrastructure. The NIPC has identified the food system as one of the eight critical infrastructures, and has established a public-private partnership with the food industry, called the Food Industry Information and Analysis Center (Food Industry ISAC). The NIPC provides the Food Industry ISAC with access, information and analysis, enabling the food industry to report, identify, and reduce its vulnerabilities to malicious attacks, and to recover from such attacks as quickly as possible. In particular, the NIPC identifies credible threats and crafts specific warning messages to the food industry. Further information is available at http://www.nipc.gov/ and http://www.foodisac.org/.

Finally, FDA encourages trade associations to evaluate the preventive measures contained in this guidance document and adapt them to their specific products and operations and to supplement this guidance with additional preventive measures when appropriate. FDA welcomes dialogue on the content of sector specific guidance with appropriate trade associations.

Retail Food Store and Food Service Establishment Operations:

Management
FDA recommends that retail food store and food service establishment operators consider:

Preparing for the possibility of tampering or other malicious, criminal, or terrorist events

- assigning responsibility for security to knowledgeable individual(s)
- conducting an initial assessment of food security procedures and operations, which we recommend be kept confidential
- having a crisis management strategy to prepare for and respond to tampering and other malicious, criminal, or terrorist actions, both threats and actual events, including identifying, segregating and securing affected products
- planning for emergency evacuation, including preventing security breaches during evacuation
- becoming familiar with the emergency response system in the community
- making management aware of 24-hour contact information for local, state, and federal police/fire/rescue/health/homeland security agencies
- making staff aware of who in management they should alert about potential security problems (24-hour contacts)
- promoting food security awareness to encourage all staff to be alert to any signs of tampering or malicious, criminal, or terrorist actions or areas that may be vulnerable to such actions, and to report any findings to identified management (for example, providing training, instituting a system of rewards, building security into job performance standards)
- having an internal communication system to inform and update staff about relevant security issues
- having a strategy for communicating with the public (for example, identifying a media spokesperson, preparing generic press statements and background information, and coordinating press statements with appropriate authorities)

Supervision

- providing an appropriate level of supervision to all staff, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially, new staff (for example, supervisor on duty, periodic unannounced visits by supervisor, daily visits by supervisor, two staff on duty at same time, monitored video cameras, off line review of video tapes, one way and two way windows, customer feedback to supervisor of unusual or suspicious behavior by staff)
- conducting routine security checks of the premises, including utilities and critical computer data systems (at a frequency appropriate to the operation) for signs of tampering or malicious, criminal, or terrorist actions, or areas that may be vulnerable to such actions

Investigation of suspicious activity

- investigating threats or information about signs of tampering or other malicious, criminal, or terrorist actions
- alerting appropriate law enforcement and public health authorities about any threats of or suspected tampering or other malicious, criminal, or terrorist actions

Evaluation program

- evaluating the lessons learned from past tampering or other malicious, criminal, or terrorist actions and threats
- reviewing and verifying, at least annually, the effectiveness of the security management program (for example, using knowledgeable in-house or third party staff to conduct tampering or other malicious, criminal, or terrorist action exercises and to challenge computer security systems), revising accordingly (using third party or in-house security expert, where possible), revising the program accordingly, and keeping this information confidential
- performing random food security inspections of all appropriate areas of the facility (including receiving and storage areas, where applicable) using knowledgeable in-house or third party staff, and keeping this information confidential
- verifying that security contractors are doing an appropriate job, when applicable

Human element – staff

Under Federal law, retail food store and food service establishment operators are required to verify the employment eligibility of all new hires, in accordance with the requirements of the Immigration and Nationality Act, by completing the INS Employment Eligibility Verification Form (INS Form I-9). Completion of Form I-9 for new hires is required by 8 USC 1324a and nondiscrimination provisions governing the verification process are set forth at 1324b.

FDA recommends that retail food store and food service establishment operators consider:

Screening (pre-hiring, at hiring, post-hiring)

- examining the background of all staff (including seasonal, temporary, contract, and volunteer staff, whether hired directly or through a recruitment firm) as appropriate to their position, considering candidates' access to sensitive areas of the facility and the degree to which they will be supervised and other relevant factors (for example, obtaining and verifying work references, addresses, and phone numbers, participating in one of the pilot programs managed by the Immigration and Naturalization Service and the Social Security Administration [These programs provide electronic confirmation of employment eligibility for newly hired employees. For more information call the INS SAVE Program toll free at 1-888-464-4218, fax a request for information to (202) 514-9981, or write to US/INS, SAVE Program, 425 I Street, NW, ULLICO-4th Floor, Washington, DC 20536. These pilot programs may not be available in all states], having a criminal background check performed by local law enforcement or by a contract service provider [Remember to first consult any state or local laws that may apply to the performance of such checks])

Note: screening procedures should be applied equally to all staff, regardless of race, national origin, religion, and citizenship or immigration status.

Daily work assignments

- knowing who is and who should be on premises, and where they should be located, for each shift
- keeping information updated

Identification

- establishing a system of positive identification and recognition (for example, issuing uniforms, name tags, or photo identification badges with individual control numbers, color coded by area of authorized access), when appropriate
- collecting the uniforms, name tag, or identification badge when a staff member is no longer associated with the establishment

Restricted access

- identifying staff that require unlimited access to all areas of the facility
- reassessing levels of access for all staff periodically
- limiting staff access to non-public areas so staff enter only those areas necessary for their job functions and only during appropriate work hours (for example, using key cards or keyed or cipher locks for entry to sensitive areas, color coded uniforms [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- changing combinations, rekeying locks and/or collecting the retired key card when a staff member who is in possession of these is no longer associated with the establishment, and additionally as needed to maintain security

Personal items

- restricting the type of personal items allowed in non-public areas of the establishment
- allowing in the non-public areas of the establishment only those personal use medicines that are necessary for the health of staff (other than those being stored or displayed for retail sale) and ensuring that these personal use medicines are properly labeled and stored away from stored food and food preparation areas
- preventing staff from bringing personal items (for example, lunch containers, purses) into nonpublic food preparation or storage areas
- providing for regular inspection of contents of staff lockers (for example, providing metal mesh lockers, company issued locks), bags, packages, and vehicles when on company

property (Remember to first consult any federal, state, or local laws that may relate to such inspections)

Training in food security procedures

- incorporating food security awareness, including information on how to prevent, detect, and respond to tampering or other malicious, criminal, or terrorist actions or threats, into training programs for staff, including seasonal, temporary, contract, and volunteer staff
- providing periodic reminders of the importance of security procedures (for example, scheduling meetings, providing brochures, payroll stuffers)
- encouraging staff support (for example, involving staff in food security planning and the food security awareness program, demonstrating the importance of security procedures to the staff)

Unusual behavior

- watching for unusual or suspicious behavior by staff (for example, staff who, without an identifiable purpose, stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility; remove documents from the facility; ask questions on sensitive subjects; bring cameras to work)

Staff health

- being alert for atypical staff health conditions that staff may voluntarily report and absences that could be an early indicator of tampering or other malicious, criminal, or terrorist actions (for example, an unusual number of staff who work in the same part of the facility reporting similar symptoms within a short time frame), and reporting such conditions to local health authorities

Human element – public

FDA recommends that retail food store and food service establishment operators consider:

Customers

- preventing access to food preparation and storage and dishwashing areas in the non-public areas of the establishment, including loading docks
- monitoring public areas, including entrances to public restrooms (for example, using security guards, monitored video cameras, one-way and two-way windows, placement of employee workstations for optimum visibility) for unusual or suspicious activity (for example, a customer returning a product to the shelf that he/she brought into the store, spending an unusual amount of time in one area of the store)
- monitoring the serving or display of foods in self-service areas (for example, salad bars, condiments, open bulk containers, produce display areas, doughnut/bagel cases)

Other visitors (for example, contractors, sales representatives, delivery drivers, couriers, pest control representatives, third-party auditors, regulators, reporters, tours)

- restricting entry to the non-public areas of the establishment (for example, checking visitors in and out before entering the non-public areas, requiring proof of identity, issuing visitors badges that are collected upon departure, accompanying visitors)
- ensuring that there is a valid reason for all visits to the non-public areas of the establishment before providing access to the facility - beware of unsolicited visitors
- verifying the identity of unknown visitors to the non-public areas of the establishment
- inspecting incoming and outgoing packages and briefcases in the non-public areas of the establishment for suspicious, inappropriate or unusual items, to the extent practical

Facility

FDA recommends that retail food store and food service establishment operators consider:

Physical security

- protecting non-public perimeter access with fencing or other deterrent, when appropriate
- securing doors (including freight loading doors, when not in use and not being monitored, and emergency exits), windows, roof openings/hatches, vent openings, ventilation systems, utility rooms, ice manufacturing and storage rooms, loft areas and trailer bodies, and bulk storage tanks for liquids, solids and compressed gases to the extent possible (for example, using locks, "jimmy plates," seals, alarms, intrusion detection sensors, guards, monitored video

surveillance [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- using metal or metal-clad exterior doors to the extent possible when the facility is not in operation, except where visibility from public thoroughfares is an intended deterrent (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- minimizing the number of entrances to non-public areas (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- accounting for all keys to establishment (for example, assigning responsibility for issuing, tracking, and retrieving keys)
- monitoring the security of the premises using appropriate methods (for example, using security patrols [uniformed and/or plain-clothed], monitored video surveillance)
- minimizing, to the extent practical, places in public areas that an intruder could remain unseen after work hours
- minimizing, to the extent practical, places in non-public areas that can be used to temporarily hide intentional contaminants (for example, minimizing nooks and crannies, false ceilings)
- providing adequate interior and exterior lighting, including emergency lighting, where appropriate, to facilitate detection of suspicious or unusual activity
- implementing a system of controlling vehicles authorized to park in the non-public parking areas (for example, using placards, decals, key cards, keyed or cipher locks, issuing passes for specific areas and times to visitors' vehicles)
- keeping customer, employee and visitor parking areas separated from entrances to non-public areas, where practical

Storage and use of poisonous and toxic chemicals (for example, cleaning and sanitizing agents, pesticides) in non-public areas

- limiting poisonous and toxic chemicals in the establishment to those that are required for the operation and maintenance of the facility and those that are being stored or displayed for retail sale
- storing poisonous and toxic chemicals as far away from food handling and food storage areas as practical
- limiting access to and securing storage areas for poisonous or toxic chemicals that are not being held for retail sale (for example, using keyed or cipher locks, key cards, seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state or local fire codes before making any changes])
- ensuring that poisonous and toxic chemicals are properly labeled
- using pesticides in accordance with the Federal Insecticide, Fungicide, and Rodenticide Act (for example, maintaining rodent bait that is in use in covered, tamper-resistant bait stations)
- knowing what poisonous and toxic chemicals should be on the premises and keeping track of them
- investigating missing stock or other irregularities outside a normal range of variation and alerting local enforcement and public health agencies about unresolved problems, when appropriate

Operations

FDA recommends that retail food store and food service establishment operators consider:

Incoming products

- using only known and appropriately licensed or permitted (where applicable) sources for all incoming products
- informing suppliers, distributors and transporters about FDA's food security guidance, "Food producers, processors, and transporters: Food security preventive measures guidance" and "Importers and filers: Food security preventive measures guidance," available at: http://www.access.gpo.gov/su_docs/aces/aces140.html.
- taking steps to ensure that delivery vehicles are appropriately secured
- requesting that transporters have the capability to verify the location of the load at any time, when practical
- establishing delivery schedules, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments
- supervising off-loading of incoming materials, including off hour deliveries

- reconciling the product and amount received with the product and amount ordered and the product and amount listed on the invoice and shipping documents, taking into account any sampling performed prior to receipt
- investigating shipping documents with suspicious alterations
- inspecting incoming products and product returns for signs of tampering, contamination or damage (for example, abnormal powders, liquids, stains, or odors, evidence of resealing, compromised tamper-evident packaging) or "counterfeiting" (for example, inappropriate or mismatched product identity, labeling, product lot coding or specifications, absence of tamper-evident packaging when the label contains a tamper-evident notice), when appropriate
- rejecting suspect food
- alerting appropriate law enforcement and public health authorities about evidence of tampering, "counterfeiting," or other malicious, criminal, or terrorist action

Storage
- having a system for receiving, storing and handling distressed, damaged, and returned products, and products left at checkout counters, that minimizes their potential for being compromised (for example, obtaining the reason for return and requiring proof of identity of the individual returning the product, examining returned or abandoned items for signs of tampering, not reselling returned or abandoned products)
- keeping track of incoming products, materials in use, salvage products, and returned products
- investigating missing or extra stock or other irregularities outside a normal range of variability and reporting unresolved problems to appropriate law enforcement and public health authorities, when appropriate
- minimizing reuse of containers, shipping packages, cartons, etc., where practical

Food service and retail display
- displaying poisonous and toxic chemicals for retail sale in a location where they can be easily monitored (for example, visible by staff at their work stations, windows, video monitoring)
- periodically checking products displayed for retail sale for evidence of tampering or other malicious, criminal, or terrorist action (for example, checking for off-condition appearance [for example, stained, leaking, damaged packages, missing or mismatched labels], proper stock rotation, evidence of resealing, condition of tamper-evident packaging, where applicable, presence of empty food packaging or other debris on the shelving), to the extent practical
- monitoring self-service areas (for example, salad bars, condiments, open bulk containers, produce display areas, doughnut/bagel cases) for evidence of tampering or other malicious, criminal, or terrorist action

Security of water and utilities
- limiting to the extent practical access to controls for airflow, water, electricity, and refrigeration
- securing non-municipal water wells, hydrants, storage and handling facilities
- ensuring that water systems and trucks are equipped with backflow prevention
- chlorinating non-municipal water systems and monitoring chlorination equipment and chlorine levels
- testing non-municipal sources for potability regularly, as well as randomly, and being alert to changes in the profile of the results
- staying attentive to the potential for media alerts about public water provider problems, when applicable
- identifying alternate sources of potable water for use during emergency situations where normal water systems have been compromised (for example, bottled water, trucking from an approved source, treating on-site or maintaining on-site storage)

Mail/packages
- implementing procedures to ensure the security of incoming mail and packages

Access to computer systems
- restricting access to critical computer data systems to those with appropriate clearance (for example, using passwords, firewalls)
- eliminating computer access when a staff member is no longer associated with the establishment

- establishing a system of traceability of computer transactions
- reviewing the adequacy of virus protection systems and procedures for backing up critical computer based data systems
- validating the computer security system

Emergency Point of Contact:

U.S. Food and Drug Administration
5600 Fishers Lane
Rockville, MD 20857
301-443-1240

If a retail food store or food service establishment operator suspects that any of his/her products that are regulated by the FDA have been subject to tampering, “counterfeiting,” or other malicious, criminal, or terrorist action, FDA recommends that he/she notify the FDA 24-hour emergency number at 301-443-1240 or call their local FDA District Office. FDA recommends that the operator also notify local law enforcement and public health authorities.

FDA District Office telephone numbers are listed at: www.fda.gov/ora/inspect_ref/iom/iomoradir.html